Information Operations: The Definition Debate

by

Maj Alexander Merz

What's in a Definition?

In the 5 years since Assistance Secretary of Defense for Command, Control, Communications, and Intelligence (ASD C3I) first endeavored to define Information Operations (IO) in terms relevant to the DoD, the only common ground we appear to have found is that the current definition is insufficient. Many feel the existing definition of IO is too expansive—it includes so many activities that everyone does it, and thus no one is responsible for it. Many others have argued that the current definition is too restrictive and does not express the true focus of IO. Add to this debate the maelstrom of opinions about what is a capability or "pillar" of IO, what is merely an associated activity, and who should be responsible for training, equipping, planning, coordinating, and executing what portions of IO.

The ongoing debate about the definition of IO has not stopped doctrinal development or real world necessity. The US Air Force published a brand new doctrine document in 2002 (AFDD 2-5, *Information Warfare*), and appears set to publish a revision in the next year. The US Army has completely rewritten Field Manual 100-6, *Information Operations*, renumbering it FM 3-13, in line with the joint publication on the same topic, JP 3-13. Though still in draft, FM 3-13 is already referenced by many in the field, primarily because the old manual (1996) is completely outdated. The US Navy recently initiated an effort to develop Psychological Operations (PSYOP) doctrine with TACMEMO 3-13.2-02 "Psychological Operations for Navy Planners," and the Marine Corps has added a course in IO at its Expeditionary Warfare Training Group in Norfolk. Meanwhile, the President has declared a Global War on Terror, central to which is the hitherto amorphous concept of IO, as we try to influence the hearts and minds of key populations around the world.

One must ask why it is so difficult to come to an agreement on what appears to be, at least on the surface, a relatively simple idea. The answer to this question, however, has proven as elusive and complex as the definition itself. It is not the purpose of this paper to resolve the joint definition of IO, but simply to shed some light on how the DoD has viewed IO over the last several years and attempt to draw some relationships that clarify how IO fits into the DoD mission.

As we begin it is instructive to recall the familiar parable of the seven blind men and the elephant. Each man's concept of the elephant was shaped by his own "reality"—that is, by the specific part of the elephant with which the man had direct contact. The man holding the leg thought he had a tree; the man holding the tail thought he possessed a rope; and so on. In a certain sense the same can be said for how different elements of the DoD have viewed IO over time. The unique missions of each of the services give rise to different problem sets and different perspectives, which lead them to emphasize different aspects of the same large concept—IO. These differences are evident in their chosen definitions and doctrine, but have added to the confusion and debate over the definition of the term overall. To better understand this debate, let us examine the evolution of the definition of IO.

The Evolution of IO

In 1998, ASD C3I, the office of primary responsibility for IO policy within the DoD, published DoD Directive S3600.1, with the following definitions related to IO:

> **INFORMATION**—1. Facts, data, or instructions in any medium or form. 2. The meaning that a human assigns to data by means of the known conventions used in their representation. (JP 1-02)
>
> **INFORMATION SUPERIORITY**—that degree of dominance in the information domain which permits

Reprinted from *Information Operations: The Definition Debate*, Air Force Special Operations University Staff Paper, July 2003, 9 pp.

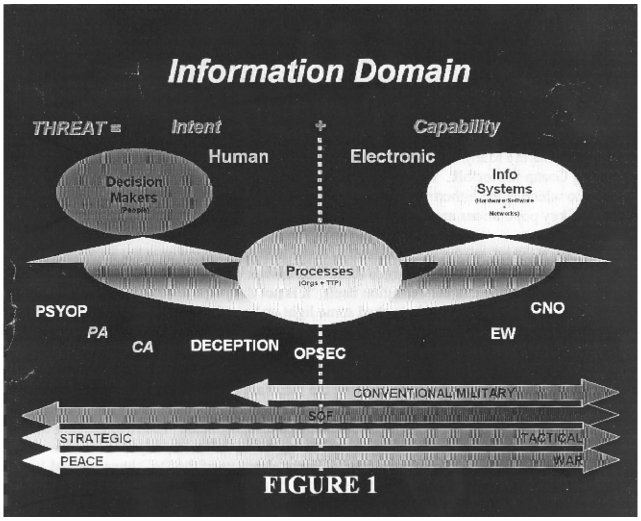

FIGURE 1

> the conduct of operations without effective opposition. (JP 1-02)

At this point we must pause to ask what is meant by the term "information domain." Of all the nebulous, unquantifiable terms in the DoD lexicon, this must be among the worst. Though we could spend months debating even this, for the sake of this discussion let us propose that the information domain consists of: 1) people (i.e. decision makers); 2) systems (i.e. machines and networks that process data); and 3) the processes that tie the first two together (i.e. organizational structures, tactics, techniques, and procedures). See figure 1. This domain spans the spectrum from interpersonal relationships to geo-strategic politics.

The information domain has taken on such importance that it has been added to the Clauswitzian concept of state power to come up with what we call the DIME—the diplomatic, *informational*, military, and economic instruments of national power. It is important to observe, however, that information can only be an instrument of national power insomuch as it relates to one of the other three. Consider the world's foremost expert on tulips. At a flower convention, this individual wields considerable power. But at a car rally he has virtually no influence, because the information he possesses is irrelevant to the automotive industry. So it is with national influence—the only information that gives a nation sway is that which relates directly to diplomacy, economics, or military might.

Continuing with our examination of the information domain, it is easy to see from figure 1 that there are two general aspects to the information domain—a human factors aspect and a technical aspect. The former includes factors such as personality, language, culture, religion, formal and informal relationships, information gatekeepers, etc. The latter includes processors, radios, sensors, satellites, networks, software, etc. This dichotomy of the information domain can be annotated by drawing an imaginary line between "People" and "Systems" and through "Processes."

With these observations, let us return to our discussion of definitions. In DoDD S3600.1, ASD C3I went on to define IO and Information Warfare (IW) as follows:

> **INFORMATION OPERATIONS**—those actions taken to affect an adversary's information and information systems while defending one's own information and information systems. (JP 1-02)
>
> **INFORMATION WARFARE**—Information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries. (JP 1-02)

As mentioned before, one's perspective shapes the emphasis one puts on a given idea. It is quickly apparent here that the perspective of ASD C3I and those who reviewed and concurred with their definition of IO in 1998, led them to emphasize the right (systems) side of figure 1.

In keeping with doctrinal protocol, the Air Force applied the joint definition of IO to 2002 service doctrine (AFDD 2-5), but with some caveats:

> **INFORMATION OPERATIONS**—those actions taken to affect an adversary's information and information systems while defending one's own information and information systems. (JP 1-02) **The Air Force believes that in practice a more useful working definition is: [*Those actions taken to gain, exploit, defend, or attack information and information systems and include both information-in-warfare and information warfare.*]**
>
> **INFORMATION-IN-WARFARE** (IIW)—IIW is a set of information operations functions that provides commander's battlespace situational awareness across the spectrum of conflict and range of air and space operations. IIW functions involve the Air Force's extensive capabilities to provide awareness throughout the range of military operations based on **integrated intelligence, surveillance, and reconnaissance (ISR) assets; its information collection/dissemination activities; and its global navigation and positioning, weather, and communications capabilities.**
>
> **INFORMATION WARFARE (IW)**—Information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries. (JP 1-02) **The Air Force believes that, because the defensive component of IW is always engaged, a better definition is: [*Information operations conducted to defend one's own information and information systems, or to attack***

***and affect an adversary's information and information systems*.]**

> **INFORMATION OPERATIONS**—Continuous military operations within the military information environment that **enable, enhance, and protect the friendly force's ability to collect, process, and act on information to achieve an advantage** across the full range of military operations; information operations include interacting with the global information environment and exploiting or denying an adversary's information and decision capabilities.

In a very restrictive approach, this old definition is internally focused on information superiority, emphasizing the middle (processes) and right (systems) portions of figure 1. The new definition, proposed in the draft FM 3-13 reads as follows:

> **INFORMATION OPERATIONS**—Army actions taken to affect adversaries' and **influence others' decision making processes,** information, and information systems while protecting one's own information and information systems.
>
> **IO Elements**—OPSEC, PSYOP, Counter Propaganda, Deception, Counter Deception, EW, CNA, IA, CND, Physical Destruction, Physical Security, Counter Intelligence.

Though still emphasizing the middle and left portions of figure 1, here for the first time we see the suggestion of influencing decisions within the scope of IO—a nod to the human factors side of the information domain. The new Army pub specifies the IO elements, choosing to leave out those things the Air Force calls IIW. Also unlike the Air Force, the Army considers all the elements as a single group of capabilities that can be applied in an offensive or defensive manner.

With the previous publication approaching 5 years old, and the debate over the definition of IO continuing, ASD C3I once again undertook to define terms for the DoD in 2002, with draft DODD 3600.1, this time unclassified:

> **INFORMATION OPERATIONS (IO)**—Actions taken to influence, affect or defend information, information systems and **decision-making**.

In the draft DODD 3600.1 ASD C3I specified that information systems here refers to both systems and processes. And so we finally see a definition of IO that encompasses the entire information domain. In addition, ASD C3I identified a select group of activities to be associated with IO. According to the draft, PSYOP, Deception, and OPSEC are core influence capabilities. EW and Computer Network Operations (CNO) are core electronic [systems] capabilities. Counter intelligence, Information Assurance, Physical Attack and Physical Security are merely supporting capabilities. Public Affairs and Civil Affairs are classed as related capabilities. It is important to note here that when ASD C3I attempted to coordinate this draft, all four services non-concurred, primarily due to differences over what capabilities should be included under the umbrella of IO. As we have seen, the Army and especially the Air Force take a broader view of what should be part of IO. Still, it is encouraging to see a definition that fully recognizes the entire information domain.

A few months after the draft of DODD 3600.1 was released, the IO roadmap, being drafted by OASD (P) initially came available, also in draft form, with the following evolution in the definition of IO:

> **INFORMATION OPERATIONS (IO)**—The employment of the core capabilities of Electronic Warfare, Computer Network Operations, PSYOP, Military Deception and Operations Security, in concert with specified supporting and related capabilities, to affect or defend information and information systems, and to influence **decision-making**.

By the summer of2003, this definition further evolved to:

> **INFORMATION OPERATIONS (IO)**—The integrated employment of the core capabilities of Electronic Warfare, Computer Network Operations, PSYOP, Military Deception and Operations Security, in concert with specified supporting and related capabilities to disrupt, corrupt or usurp adversarial human and automated **decision-making** while protecting our own.

These adjustments in wording reveal the tensions at the policy level between making IO broad enough to address the information domain, while ensuring that the DoD stays within its assigned roles within the U.S. Government. It also recognizes the fact that, as systems become more and more advanced, they themselves become limited decision makers, in some cases blurring the lines in the information domain between systems and decision makers. It remains to be seen whether this latest definition will endure.

Affecting Actions—The Essence of IO

With this examination of the definition debate behind us, it is instructive to explore in more detail how the information domain works in order to understand differences in service doctrine on the subject. The question arises, when considering the information domain, how one can affect it. Here it seems best to consider how humans interact with the information domain. See figure 2. There exists a universe of facts—things that are true at any given time. The number of tanks in the Iraqi inventory, the state of the rainforest in Guatemala, the number of people in Antarctica, what President Bush thinks about Tony Blair, what Tony Blair thinks President Bush thinks about him, etc, etc, are all pieces of this universe. This universe is dynamic—constantly changing with time. From it, we collect bits and pieces via a variety of "sensors"—eyes, ears, satellites, thermometers, etc, etc. These factoids are stored as *Information* by any number of means, electronic, mechanical, human, and otherwise. At some point, certain portions of this information are organized, correlated, processed and communicated to individuals or systems in a meaningful way, at which point the information becomes *knowledge*, or actionable data, for that individual or system. Humans and automated systems then take this knowledge, and make decisions about what actions to take, based on cultural, biological, emotional, algorithmic filters unique to each actor. As mentioned, actors may be people *or in some cases* automated systems capable of making decisions when given certain inputs.

This process occurs at multiple levels from interpersonal to international, in a continuous cycle. Those in the military are most familiar with it under the term "OODA Loop"—Observe, Orient, Decide, Act. The ultimate aim of any attempt to affect this process is to bring about a desired *Action* on the part of the target actor. One can affect this process in a variety of ways. One can increase the number of facts available in certain areas, while decreasing or eliminating the flow of facts in others. At other times it may be more useful to shape, filter, or "spin" available facts to make them seem more or less significant, or to present certain falsehoods as facts. In addition, one can affect target actor knowledge, by influencing how information is processed and communicated—controlling what bits of information are processed, affecting how they are interpreted, influencing the weight or trust placed in a given bit of information, or interfering with/adding to the communication process. Once actors make decisions based on the knowledge they have received, one can affect how those decisions are communicated … and the cycle continues.

Returning then to the definition debate, one could say that IO is the attempt to protect one's own decision process, with its resulting actions, while affecting the decision processes of other actors to achieve those actions which are most desirable. In a sense, we all conduct IO at the personal level every day. On performance evaluations we increase, filter, and "spin" the good information and minimize the less complementary details, all to bring about a desired action by the promotion boards. When returning home late from work we emphasize the facts that we were working on an important project with other co-workers, and minimize the facts that we spent most of our time telling jokes over coffee, and the project wasn't due until next month. The desired action we seek on the part of our spouse is an acceptance of our tardy appearance as excusable. The means we use will change based on the circumstances, but the objective, whether personal or national strategic, is always to affect the resulting actions of others.

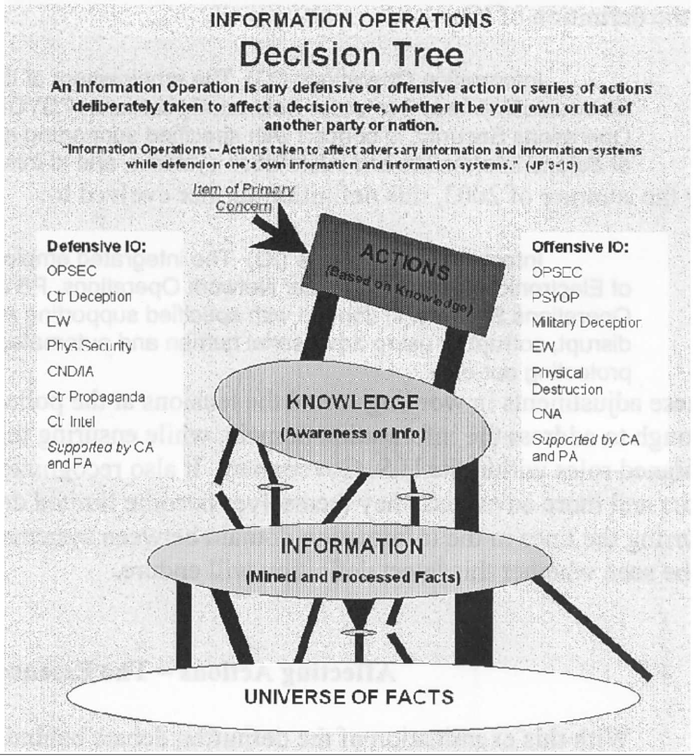
INFORMATION OPERATIONS
Decision Tree
An Information Operation is any defensive or offensive action or series of actions deliberately taken to affect a decision tree, whether it be your own or that of another party or nation.
"Information Operations -- Actions taken to affect adversary information and information systems while defendion one's own information and information systems." (JP 3-13)
Item of Primary Concern
ACTIONS
(Based on Knowledge)
Defensive IO:
OPSEC
Ctr Deception
EW
Phys Security
CND/IA
Ctr Propaganda
Ctr Intel
Supported by CA and PA
Offensive IO:
OPSEC
PSYOP
Military Deceptior
EW
Physical Destruction
CNA
Supported by CA and PA
KNOWLEDGE
(Awareness of Info)
INFORMATION
(Mined and Processed Facts)
UNIVERSE OF FACTS

Figure 2

Here once again we can make some interesting observations. In general one can say that, defensive IO aside, on the spectrum of conflict, during peacetime IO is limited primarily to the left side of figure 1—targeting human thoughts and thought processes. As we move across the spectrum toward war more options become available on the technical side of the domain. Electronic Warfare (EW) and Computer Network Attack (CNA) are almost exclusively conducted during wartime. During peacetime, PSYOP programs and public information are the primary tools of the information warrior.

In addition, when we think about a given threat, we commonly break it down into two components—1) the capability to inflict injury and 2) the intent to inflict injury. Without both components no threat exists. If we overlay this on the information domain, we find that intent resides in the human factors portion, and capability resides in the systems portion of the domain.

The logical extension of these two points is that for IO to be used effectively in scenarios short of war, and thus successfully avoid war, we must have mature and well coordinated strategic PSYOP and public information programs/capabilities. In the absence of this, we are left solely with the costly option of securing our nation by repeatedly destroying the capability behind every threat in crisis situations, rather than preempting the crisis by addressing intentions. To some degree, the conventional military focus has led us down exactly this path—concentrating on the capability of every possible threat, while largely ignoring the associated intent.

A Matter of Perspective

Thus we revisit the point made at the beginning regarding perspectives. One's approach to IO may vary widely depending on scope and focus of mission. Consider a situation in which we are trying to stop a tank from driving into a town square and annihilating the population of innocent civilians. Aside from the obvious kinetic solution of blowing up the tank, there are a variety of information options available. At the tactical level, the friendly force A Team commander on the ground may use a tactical jammer to stop the tank from receiving orders. He may attempt to send false orders, rearrange road signs to confuse the tank driver, or prevent the tank crew from seeing where it is going, so it will never get to the village. In addition, he may attempt to deter the tank crew from wanting to go to the village, through the threat of lethal retaliation or causing them to connect emotionally with the occupants of the village. His options are limited in time and scope and tend toward the right side of figure 1.

At the operational level the JTF commander, in order to stop the tank, may conduct IO to interrupt the adversary logistics systems and stop the flow of fuel, spare parts, and munitions to the tank. He may also attempt to confuse or deter the battalion or division commander of the tank, in order to change the orders sent to the tank. Alternatively, he may order actions that will divert the tank crew's attention to other higher priorities or persuade them to avoid the village. His options have a broader scope and may well require more lead time for execution than those of the A Team commander. And they will likely tend toward the middle of figure 1.

At the strategic level the President of the United States has other options at his disposal. He and his allies in other countries can communicate with national leaders of the army to which the tank belongs, threatening or persuading them to prevent the tank from attacking the village. He may also implement economic sanctions or order a show of force in the region. His options have a broad sweeping scope and usually require much more lead time to implement, tending toward the left side of figure 1.

Similarly, if we consider the service perspectives, Air Force planners look at defeating the tank first from the hard kill perspective via bomb dropping, then from the EW and interdiction perspectives—in keeping with Air Force primary missions. On the other hand, the Army looks at defeating the tank first from the hard kill perspective via one of their many tank killing options, then from the EW, tactical deception, and tactical PSYOP perspectives, again in keeping with Army primary missions. The Navy sees defeating the tank similarly to the Air Force, while the Marine Corps focuses on hard kill and EW. In summary, all the services deal with threats primarily at the operational level and below, and approach the threats from the capabilities aspect based on their own strengths and capabilities. This is the natural approach, completely consistent with JOPES and the DoD mission to "support and defend the constitution of the United States against all enemies, foreign and domestic." On the other hand, SOCOM, though not a service, but with service-like responsibilities, brings a unique perspective to the IO landscape. With forces engaged in over 80 countries at any given time working routinely with State Department and other government agencies, special operations forces (SOF) have a more strategic focus. The DoD's PSYOP capability, a key element of the human factors side of IO, resides almost exclusively within SOCOM. These facts uniquely qualify SOCOM to engage in IO across the spectrum from peace to war and strategic to tactical.

That said, the problem we have encountered, which has been illustrated and pointed out on multiple occasions in the last few years, is that the U.S. as a whole has largely neglected IO above the operational level. Theater Security Cooperation (TSC) planning, formerly Theater Engagement planning, is a relatively recent, yet limited attempt by the DoD to go beyond the operational level. But TSC planning has received very little attention in many cases. Even PSYOP units have largely been resource constrained and restricted to doing tactical-operational level products. As a result Secretary Rumsfeld, in the latest Defense Planning Guidance (DPG), singled out strategic influence as a key shortfall in DoD capabilities and directed SOCOM to pursue strategic PSYOP capabilities. The challenge is that the DoD is not the only player in IO, particularly above the operational level. There are many other stake holders and key actors within the DIME. The DoD can not be the lead agency in strategic peacetime IO. But DoD involvement is essential, which is why the DPG directed the DoD to give conscious thought to who, what, when and how the DoD should approach it.

Should SOCOM be the lead agency for IO in the DoD? STRATCOM? The chip seems to be falling toward STRATCOM. Given our discussion above, this is a logical decision, though it would seem SOCOM might be a better fit in many ways. That aside a host of other questions remain about what capabilities should be included under the term IO, who should be responsible to train and equip which pieces, and who has operational control in what circumstances. As we sort through these questions, we would do well to observe the different perspectives of the services and government agencies and make decisions that respect these differences while meeting the unique requirements of operationalizing IO within the DoD. The solution that seems to be falling out naturally is that STRATCOM will take the overall lead in coordinating and sponsoring IO within the DoD, while SOCOM focuses on the human factors portion of the problem and the services address the systems portion of the problem. Given our discussion above, this may work quite well in the end.

Forging Ahead

In conclusion, the debate over the definition of IO continues on, driven by differing perspectives on such a large topic. If, however, we take the time to explore the concepts and relationships surrounding IO, it appears these differing perspectives are not necessarily contradictory, but may only reflect different emphases based on the strengths and weaknesses of those involved. The definition we choose must strike a balance between allowing primary participants the freedom to operationalize IO from their perspective, while being specific enough to provide focused unity of effort across the DoD. Perhaps we are closer to achieving this than we realize. In any case, the significance of IO will likely only expand as our world increasingly exploits the information domain.